SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Marko Katanović

USPOREDBA ZNAČAJKI PROTOKOLA MREŽNOG SLOJA TCP/IP SKUPINE PROTOKOLA I NJIHOVE PRIMJENE

ZAVRŠNI RAD

Zagreb, 2015.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

USPOREDBA ZNAČAJKI PROTOKOLA MREŽNOG SLOJA TCP/IP SKUPINE PROTOKOLA I NJIHOVE PRIMJENE

A COMPARISON OF TCP/IP NETWORK LAYER PROTOCOL CHARACTERISTICS AND THEIR APPLICATIONS

Mentor: dr.sc. Marko Matulin

Student: Marko Katanović, 0135221987

Zagreb, 2015.

SAŽETAK

OSI (*Open Systems Interconnection*) referentni model osigurava stručnjacima i proizvođačima temelj na kojem proučavaju mrežu i sve njezine elemente i procese kroz taj sedmoslojni apstraktni model. Na TCP/IP (*Transmission Control Protocol/Internet Protocol*) modelu zasniva se internetska arhitektura koja je opisana kroz svoja četiri sloja. Posebno je opisan drugi sloj ovog modela, internet sloj. Analiza ovog sloja pokazala je koje se funkcije i procesi izvršavaju, kako djeluje enkapsulacija podataka te koji protokoli obilježavaju procese ovog sloja. Opisani su kontrolni protokoli, protokoli razlučivanja adrese, protokoli usmjeravanja i internet protokol sa svoje dvije verzije.

KLJUČNE RIJEČI: OSI referentni model; TCP/IP model; protokoli; mrežni sloj

SUMMARY

OSI (*Open Systems Interconnection*) reference model provides experts and manufacturers the basis on which they study the network and all its elements and processes through that seven-layer abstract model. On the TCP/IP (*Transmission Control Protocol/Internet Protocol*) model is based the Internet architecture which is described through its four layers. Particularly described is the second layer of the model, the Internet layer. The analysis of this layer revealed which functions and processes perform, how the encapsulation of data works and which protocols characterize the processes of this layer. Control protocols, address resolution protocols, routing protocols and Internet protocol with its two versions are described.

KEYWORDS: OSI reference model; TCP/IP model, protocols, internet layer

SADRŽAJ

1. Uvod

Razvojem računalne mreže, Interneta, stručnjaci su razvili osnovne TCP/IP (*Transmission Control Protocol/Internet Protocol*) protokole nakon što je mreža postala operativna. Razvijen je TCP/IP model na kojem se zasniva internetska arhitektura, te se kroz njega proučava, razvija i nadograđuje. Mrežni sloj, jedan od četiri sloja ovog modela ima zadaću pružanja usluge povezanosti i odabira najbolje rute za slanje podataka kroz mrežu. Naslov završnog rada je: Usporedba značajki protokola mrežnog sloja TCP/IP skupine protokola i njihove primjene. Rad je podijeljen u sedam cjelina:

1. Uvod
2. OSI referentni model
3. Internet protokolni složaj i relacija s OSI referentnim modelom
4. Enkapsulacija podataka
5. Protokoli mrežnog sloja TCP/IP složaja
6. Komparacija IPv4 i IPv6 usmjeravanja
7. Zaključak

U drugom poglavlju je opisan OSI referentni model i sve njegove karakteristike i procesi. Ukratko je opisano svih sedam slojeva ovog modela.

Treće poglavlje obuhvaća TCP/IP model, te su opisana njegova četiri sloja s protokolima i funkcijama koje ti slojevi obnašaju. Opisana je sličnost i razlika TCP/IP modela i OSI referentnog modela.

U četvrtom poglavlju prikazana je enkapsulacija podataka, proces prijenosa podataka s predajne strane od pošiljatelja do cilja, odnosno primatelja.

Peto poglavlje obuhvaća protokole mrežnog sloja TCP/IP složaja koji su podijeljeni na četiri grupe protokola, a to su: kontrolni protokoli, protokoli razlučivanja adrese, protokoli usmjeravanja i internet protokol kao najvažniji protokol na ovom sloju.

Šesto poglavlje opisuje komparaciju između dvije verzije internet protokola, IPv4 i IPv6 te njihove karakteristike, prednosti i nedostatke, te sličnosti i razlike.

2. OSI referentni model

Rani razvoj LAN (*Local Area Network*), MAN (*Metropolitan Area Network*) i WAN (*Wide Area Network*) mreža osamdesetih godina prošlog stoljeća bio je loš u mnogim pogledima. Tih godina povećao se broj i veličina mreža, te su mnoge velike kompanije shvaćale da umrežavanjem povećavaju svoju dobit, a smanjuju troškove. Tako su se dodavale i gradile nove mreže i povećavale postojeće, ali nakon nekoliko godina su se polako počele osjećati poteškoće zbog učinjenih proširenja. Postajalo je sve teže da te mreže međusobno komuniciraju jer su koristile različite specifikacije i implementacije, a ljudi koji su u velikim kompanijama bili zaduženi za razvoj mreže i umreživanja uvidjeli su da svoj rad moraju usmjeriti prema otvorenim rješenjima i odbaciti razmišljanja od zatvorenih rješenja. Do tada je svaka velika kompanija imala svoj način i drugačiji razvoj, koji je bio međusobno nepoveziv i nekompatibilan. Da bi se to pitanje rješilo Međunarodna organizacija za standardizaciju (*International Organization for Standardization - ISO*) istraživala je različite načine i mrežne sheme, te je stvoren mrežni model koji je trebao pomoći proizvođačima mrežne opreme da stvori mreže koje će biti u mogućnosti funkcionirati s ostalim mrežama. Tako je nastao OSI referentni model.[1]

OSI referentni model (*Open Systems Interconnection Reference Model* – OSI RM) ili referentni model za otvoreno povezivanje sustava je apstraktni, slojeviti model koji služi kao preporuka stručnjacima za razvoj računalnih mreža i protokola. Ovaj model opisuje komunikaciju hardware-a i software-a, te raznih programa i protokola pri mrežnim komunikacijama. OSI model koriste proizvođači i stručnjaci pri projektiranju i proučavanju mreža, jer dijeli arhitekturu mreže na slojeve te daje spisak funkcija, usluga i protokola kako rade i funkcioniraju na svakom sloju. OSI model podijeljen je u sedam slojeva, gdje svaki sloj opisuje skup povezanih funkcija koje omogućuju jedan dio računalne komunikacije. Svih sedam slojeva zajedno funkcionira kao jedna cijelina te prikazuju tok podataka od izvora prema odredištu, od prvog do zadnjeg sloja. OSI referentni model pruža važne smjernice u razvoju mrežnih protokola. Mrežni komunikacijski protokol predstavlja skup određenih pravila koja su potrebna da bi se podaci mogli prenijeti preko komunikacijskog kanala. Dok za opis mrežne

[1] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_1_2.html

arhitekture služi OSI referentni model, za opis internetske arhitekture koristi se TCP/IP model. [2]

OSI referentni model dijeli se na sedam slojeva, kao što prikazuje slika 1, a svaki od tih slojeva opisuje određenu mrežnu funkciju:

- Aplikacijski sloj – sloj 7 (*Layer 7*)
- Prezentacijski sloj – sloj 6 (*Layer 6*)
- Sloj sesije – sloj 5 (*Layer 5*)
- Transportni sloj – sloj 4 (*Layer 4*)
- Mrežni sloj – sloj 3 (*Layer 3*)
- Podatkovni sloj – sloj 2 (*Layer 2*)
- Fizički sloj – sloj 1 (*Layer 1*)

Slika 1. Prikaz slojeva OSI referentnog modela[3]

Slojevi unutar jednog modela komuniciraju s prvim slojem iznad sebe i prvim slojem ispod sebe. Gornji sloj ovisi o funkcionalnosti koji pruža sloj ispod njega. Ukoliko se komunikacija prikaže s dva OSI modela, može se vidjeti da se slojevi jednog modela povezuju samo s istim slojevima drugog modela. Npr., mrežni sloj jednog modela povezati će se s mrežnim slojem drugog modela. Takva povezanost se naziva *peer-to-peer* komunikacija.

[2] Bažant, A., Car, Ž., Gledec, G., Jevtić, D., Ježić, G., Kunštić, M., Lovrek, I., Matijašević, M., Mikec, B., Skočir, Z.: Telekomunikacije – tehnologije i tržište, Element, Zagreb, 2007. (str. 237-238)
[3] http://www.konides.ag.rs/mreze/12-OSI/arhitektura_slojeva.html

Odvajanje slojeva naziva se *layering* (uslojavanje modela komuniciranja), a takvim procesom imamo sljedeće pogodnosti: mrežna komunikacija svedena je na manje, jednostavnije dijelove. Standardizirane su mrežne komponente koje omogućuju razvoj od više proizvođača. Moguća je komunikacija različitih tipova mrežnog hardvera i softvera, dok promjena na jednom sloju ne utječe na druge slojeve, što znači da razvoj pojedinog sloja može biti brži. Mrežna komunikacija svedena je na manje komponente zbog čega je učenje o mrežama lakše i jednostavnije.[4]

Slojevi OSI referentnog modela podijeljeni su u dvije grupe, na više i niže slojeve.

2.1. Viši slojevi

Više slojeve ili prvu grupu čine gornja tri sloja: sloj aplikacije, sloj prezentacije i sloj sesije. Viši slojevi imaju ulogu opisivanja procesa komunikacije između korisnika i računala, te rad korisnika s aplikacijom i proces komunikacije aplikacija međusobno kao krajnjim točkama. Viši slojevi su slojevi aplikacije i kao takvi su u bliskom doticaju sa samim korisnikom.

Aplikacijski sloj je sedmi i najviši sloj u OSI referentnom modelu, te kao takav najbliži korisniku. Razlikuje se od ostalih slojeva jer ne pruža usluge drugim slojevima, već pruža mrežne usluge korisničkim aplikacijama koje su smještene van OSI modela.[5] Primjeri takvih aplikacija su tablični kalkulatori i word procesori. Sedmi sloj uspostavlja i sinkronizira procedure za prijenos podataka, uspostavlja dogovore o procedurama oporavka u slučaju greški i kontrolira integritet podataka. Primjeri protokola kod sedmog sloja su: HTTP (*HyperText Transfer Protocol*), FTP (*File Transfer Protocol*), Telnet, SMTP (*Simple Mail Transfer Protocol*), POP (*Post Office Protocol*) i IMAP (*Internet Message Access Protocol*).

Prezentacijski sloj je šesti sloj u OSI referentnom modelu i njegova glavna uloga je da brine o tome da informacija koju pošalje aplikacijski sloj jednog sustava bude čitljiva od strane aplikacijskog sloja drugog sustava. Brine se o formatu i strukturi podataka i pregovara o sintaksi prijenosa za aplikacijski sloj. Podaci koji se koriste na raznim računalima se kodiraju na razne načine i na različite načine označavaju prelazak u novi red. Sve takve konverzije se izvode na

[4] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_1_2.html
[5] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_1_2.html

ovom sloju. Ako je potrebno ovaj sloj prevodi između višestrukih podatkovnih formata, koristeći zajednički format. Česti grafički standardi prezentacijskog sloja su PICT, TIFF i JPEG, a primjeri standarda za zvuk i filmove su MIDI i MPEG.

Sjednički sloj ili sloj sesije je peti sloj u OSI referentnom modelu, zadužen je za uspostavu, upravljanje i prekid veze između krajnjih korisnika, odnosno između dva računala koja komuniciraju. Bitna zadaća ovog sloja je sinkronizacija dijaloga između prezentacijskih slojeva dvaju računala i upravljanje razmjenom podataka između njih. Sloj upravlja kontrolom veze, te nudi kakvoću usluge i obavještava o problemima unutar aplikacijskog, prezentacijskog i sloja sesije. Primjeri protokola sloja sesije su: NFS (*Network File System*) i ASP (*AppleTalk Session Protocol).*

2.2. Niži slojevi

Niže slojeve ili drugu grupu čine četiri donja sloja: transportni sloj, mrežni sloj, podatkovni sloj i fizički sloj. Niži slojevi nam opisuju i prikazuju procese kako se prenose informacije od jednog do drugog korisnika.

Transportni sloj je četvrti sloj u OSI referentnom modelu, a njegova funkcija je da na pouzdan način prenese podatke između uređaja. Sekundarna zadaća mu je da otkrije i ispravi greške u prijenosu. Ako dođe do pogrešnog ili nepotpunog slanja podataka, transportni sloj traži da se slanje ponovi. Transportni sloj uspostavlja, održava i prekida virtualne krugove, kao što je telefonski poziv. Proces radi na način da korisnik bira broj, uspostavlja vezu i priča sa sugovornikom. Za cijelo vrijeme trajanja poziva između njih postoji virtualni komunikacijski kanal, a nakon završetka razgovora jedan od sugovornika prekida vezu, te se time automatski prekida i virtualni kanal.[6] Primjeri protokola transportnog sloja su: TCP i UDP. TCP (*Transmission Control Protocol*) je konekcijski protokol koji radi na način da kreira virtualnu konekciju od jednog hosta do drugog te tako prenosi podatke. On je spojni protokol koji garantira pouzdanu, ali sporiju isporuku podataka, koja je kontrolirana od pošiljatelja s jedne strane do primatelja na drugoj strani, dok je UDP (*User Datagram Protocol*) protokol bezkonekcijski. UDP je protokol koji omogućuje slanje kratkih datagrama. Brži je i efikasniji od TCP-a, ali je nepouzdan iz razloga jer ne provjerava pogreške prilikom slanja podataka.

[6] http://sistemac.carnet.hr/node/352

Nema mogućnost provjere primitka poruke na strani primatelja jer radi na principu „pošalji i zaboravi“.

Mrežni sloj je treći sloj u OSI referentnom modelu koji ima zadaću pružiti uslugu povezanosti i odabrati najbolju rutu za paket podataka kroz mrežu, budući da podaci od pošiljatelja do primatelja mogu putovati mrežom različitim rutama. Uz funkciju uspostavljanja, održavanja i raskida veze, obavlja još niz funkcija, kao što je dodatno segmentiranje IP paketa na manje segmente, te prevođenje logičkih adresa u MAC adrese. Sloj upravlja s adresiranjem poruke, a najvažnija funkcija koju obavlja je usmjeravanje, za što su zaduženi uređaji koji se zovu usmjernici (*routeri*). Primjer protokola mrežnog sloja je Internet Protocol (IP).

Podatkovni sloj je drugi sloj u OSI referentnom modelu. On omogućuje pouzdan prijenos podataka preko medija i brine se o relevantnom pristupu mediju za prijenos podataka. Bavi se pitanjima fizičkog adresiranja, mrežne topologije, obavještavanju o greškama, uređene dostave okvira i kontrole protoka.[7] Podatkovni sloj je podijeljen na dva dijela: LLC i MAC. Kontrola logičke veze (*Logical Link Control* – LLC) osigurava kontrolu greške te komunicira s mrežnim slojem radi uspostave i načina veze, odnosno hoće li ona biti konekcijska ili bezkonekcijska. Kontrola pristupa mediju (*Media Access Control* - MAC) komunicira s fizičkim slojem te pruža pristup LAN mediju.

Fizički sloj je prvi sloj u OSI referentnom modelu ispod kojeg nema više slojeva, već pasivno okruženje, te se zbog toga razlikuje od drugih slojeva. Ovaj sloj brine o fizičkim komponentama mreže, kao što su konektori, razine napona i signala, brzine prijenosa podataka, te mediji za prijenos.[8] Ovaj sloj definira procese za uspostavu, održavanje i raskid fizičkog linka između krajnjih sustava.

[7] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_1_2.html
[8] http://sistemac.carnet.hr/node/352

3. Internet protokolni složaj i relacija s OSI RM

Godine 1969. istraživačka agencija Ministarstva obrane SAD-a (*Department of Defense - DoD*) naziva DARPA (*Defense Advanced Research Projects Agency*) koja je razvijala nove tehnologije za vojsku SAD-a, uključujući računalne mreže, razvila je mrežu imena ARPANET, koja je kasnije prerasla u Internet. Mnoge tehnike moderne komunikacije podataka razvijene su u toj mreži. Bila je to velika rasprostranjena mreža koja je služila kao osnova za testiranje novih mrežnih tehnologija. Povezivala je mnoga sveučilišta i istraživačke centre, a prva dva čvora ARPANET-a bili su Sveučilište Los Angeles u Kaliforniji i Institut za istraživanja Sveučilišta Stanford. ARPANET je 1975. godine prenamijenjen iz eksperimentalne mreže u operativnu mrežu. Svejedno se nije odustalo od daljnjeg razvoja mreže, te su osnovni TCP/IP protokoli razvijeni nakon što je mreža postala operativna. TCP/IP protokoli su usvojeni kao vojni standardi (*Military Standards* – MIL STD) 1983. godine, te svi hostovi koji su htjeli biti spojeni na mrežu morali su prilagoditi svoje standarde ovoj skupini protokola. U vrijeme kada je TCP/IP prihvaćen kao standard, termin „Internet“ prihvaćen je kao naziv u svakodnevnoj uporabi.[9]

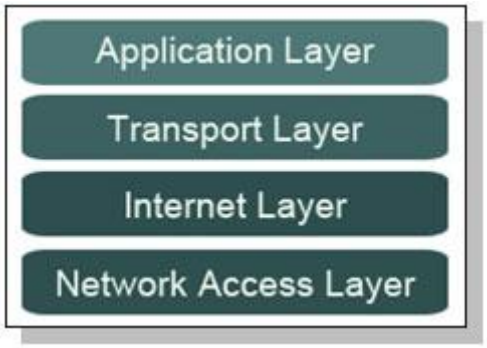
Dok OSI referentnim modelom na apstraktan način možemo promatrati mrežnu arhitekturu, koristeći slojeviti prikaz kod kojeg svaki sloj koristi usluge nižih i pruža usluge višim slojevima, TCP/IP model nam detaljno prikazuje internetsku arhitekturu.

3.1. TCP/IP model

Model TCP/IP također slijedi načelo slojevitosti, ali se razlikuje po broju slojeva i po smještaju pojedinih funkcija po slojevima. Dok OSI referentni model ima sedam slojeva, TCP/IP model ima četiri sloja, a to su: sloj podatkovne veze, mrežni sloj, transportni sloj i aplikacijski sloj, kao što se vidi na slici 2. U literaturi mogu se naći razne podjele, a činjenica da ovaj model pokriva iste funkcije kao i OSI model, preslikavanje funkcija nije isto po slojevima. TCP/IP protokol prisutan je danas na skoro svim računalima, posebno zbog mogućnosti povezivanja na Internet, te razloga da svaki sloj ima drugačiju strukturu podataka.

[9] Hunt, C.: TCP/IP Network Administration, O'Reilly Media, 1997.

Na aplikacijskom sloju TCP protokol za podatke koristi naziv tok (*stream*), dok se kod UDP protokola koristi naziv poruka (*message*). TCP na prijenosnom sloju naziva podatke segment, a UDP paket. Na mrežnom sloju svi podaci su predstavljeni datagramom, a na sloju podatkovne veze okvirom.



Slika 2. Prikaz slojeva TCP/IP modela[10]

3.1.1. Sloj podatkovne veze

Sloj podatkovne veze je prvi sloj kod TCP/IP modela jer se fizički sloj kao neki temeljni „nulti“ sloj može temeljiti na bilo kojem standardu. Internetska arhitektura fizički sloj pretpostavlja ali ga ne obrađuje kao zasebnu cjelinu. Protokoli ovog sloja zaduženi su za dostavu podataka na druge uređaje koji su direktno povezani na mrežu, te definiraju kako iskoristiti mrežu za prijenos IP datagrama. Ovaj sloj kod TCP/IP modela može zamijeniti i nadomjestiti sve funkcije i uloge kod nižih slojeva OSI referentnog modela i to kod fizičkog, podatkovnog i mrežnog sloja. Kako se stalno pojavljuje nova hardware tehnologija, novi protokoli ovog sloja moraju biti razvijeni tako da bi uređaji koji se zasnivaju na TCP/IP modelu mogli koristiti tu hardware tehnologiju. Funkcije koje se izvode na toj razini uključuju enkapsulaciju IP datagrama u okvire koji se prenose mrežom, te mapiranje IP adresa u fizičke adrese koje koristi mreža. Protokoli na ovom sloju često se pojavljuju kao kombinacija „*drivera*“ i povezanih, srodnih programa.[11]

[10] https://www.certificationkits.com/cisco-certification/ccna-articles/cisco-ccna-standard internetworking-models/ccna-the-tcpip-suite/
[11] Hunt, C.: TCP/IP Network Administration, O'Reilly Media, 1997.

Sloj podatkovne veze kod TCP/IP modela uključuje LAN i WAN protokole, te sve detalje, funkcije i procese koji su uključeni u fizički i podatkovni sloj, odnosno prvi i drugi sloj OSI referentnog modela.

Tehnike i protokoli kod ovog sloja TCP/IP modela su: Ethernet, ATM (*Asynchronus Transfer Mode*) i *Frame relay* koji nam služe za prijenos podataka.

3.1.2. Mrežni sloj

Mrežni sloj ili internet sloj je drugi sloj kod TCP/IP modela, a njegove osnovne funkcije su adresiranje i usmjeravanje. Zadaća mrežnog sloja je ostvariti nespojnu vezu između mrežnih sučelja. Mrežni sloj uz mrežne protokole sadrži i kontrolne protokole i protokole usmjeravanja. Najvažniji kontrolni protokol je ICMP (*Internet Control Message Protocol*) koji djeluje kada u mreži dođe do neočekivanih događaja. Kod ovog sloja važna su još dva protokola, ARP (*Address Resolution Protocol*) i RARP (*Reverse Address Resolution Protocol*). Oni vrše međusobno preslikavanje između IP adrese i fizičke adrese sučelja.[12]

Osnovni i najvažniji protokol ovog sloja je IP (*Internet Protocol*), koji služi za prijenos podataka. IP pruža osnovnu uslugu dostave paketa na kojoj je TCP/IP model napravljen. Svi protokoli koje koristi mrežni sloj koriste IP za dostavu podataka. IP protokol je nepouzdan budući da radi na modelu usluge koji se naziva „najbolji mogući“ (*best effort*), što znači da nema nikakve potvrde da će paket koji je poslan od pošiljatelja zaista i doći do strane primatelja.

Funkcije ovog protokola su da definira datagram, definira shemu adresiranja na Internetu, prebacuje podatke između prvog i trećeg sloja, odnosno između sloja podatkovne veze i transportnog sloja, te vrši usmjeravanje datagrama do udaljenih računala.[13]

3.1.3. Transportni sloj

Transportni sloj ili treći sloj TCP/IP modela brine se o kvaliteti usluge, problematici pouzdanosti, protoku podataka i ispravljanju grešaka. Njegova funkcija je da ostvari potporu

[12] Bažant, A., Car, Ž., Gledec, G., Jevtić, D., Ježić, G., Kunštić, M., Lovrek, I., Matijašević, M., Mikec, B., Skočir, Z.: Telekomunikacije – tehnologije i tržište, Element, Zagreb, 2007.
[13] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_3.pdf

komunikaciji između procesa, uz mogućnost da otkrije i ispravi pogrešku, te da upravlja tokom prema zahtjevima aplikacije.

Ovaj sloj predstavlja vezu u komunikaciji između mrežnog i aplikacijskog sloja. Mrežni sloj iz svog zaglavlja saznaje kojem protokolu transportnog sloja treba predati podatke, a transportni sloj na osnovu podataka u svom zaglavlju te podatke prosljeđuje točno određenoj usluzi aplikacijskog sloja. Postoje dva osnovna načina prijenosa podataka na ovom sloju, a to su: s uspostavom logičkog kanala i bez uspostave logičkog kanala. Izbor o načinu prijenosa podataka ovisi o tipu i veličini poruke. Prijenos s uspostavom logičkog kanala je spojni način koji osigurava pouzdanu isporuku podataka do odredišta uz što manje gubitaka i što manje pogrešaka, te se primjenjuje kod prijenosa korisničkih podataka. Drugi način je prijenos bez uspostave logičkog kanala, koji je bespojni, te se primjenjuje kod prijenosa upravljačkih poruka.[14]

Najvažnija dva protkola ovog sloja su TCP i UDP. TCP je protokol koji pruža spojnu i pouzdanu uslugu s kraja na kraj pomoću mehanizma potvrde i retransmisije, te čuva redoslijed datagrama. S druge strane, UDP pruža nespojnu i nepouzdanu uslugu koja ne čuva redoslijed datagrama.

3.1.4. Aplikacijski sloj

Aplikacijski sloj je četvrti te najviši sloj kod TCP/IP modela. Ovaj sloj čine programi i procesi koji svoje zahtjeve ili podatke predaju izravno protokolima transportnog sloja. Dizajneri TCP/IP modela su smatrali da protokoli višeg sloja trebaju objedinjavati detalje veze i prezentacije, te je zbog toga kreiran aplikacijski sloj koji upravlja s protokolima višeg sloja, problematikom prikaza, enkodiranjem i kontrolom dijaloga. TCP/IP kombinira svu problematiku vezanu uz aplikativni dio u aplikacijskom sloju. Primjeri usluga s odgovarajućim protokolima su: transfer datoteka (*File Transfer Protocol* - FTP), interaktivni rad na daljinu (*Telnet*), elektronička pošta (*Simple Mail Transfer Protocol* - SMTP), pregledavanje informacija (*HyperText Transfer Protocol* - HTTP) i upravljanje mrežom (*Simple Network Management Protocol* - SNMP).[15]

[14] http://tfotovic.tripod.com/ni_protokoli.htm
[15] Bažant, A., Car, Ž., Gledec, G., Jevtić, D., Ježić, G., Kunštić, M., Lovrek, I., Matijašević, M., Mikec, B., Skočir, Z.: Telekomunikacije – tehnologije i tržište, Element, Zagreb, 2007.

Neki od rijeđe korištenih i manje poznatijih protokola aplikacijskog sloja su: DNS (*Domain Name System*), RIP (*Routing Information Protocol*) i NFS (*Network File System*).

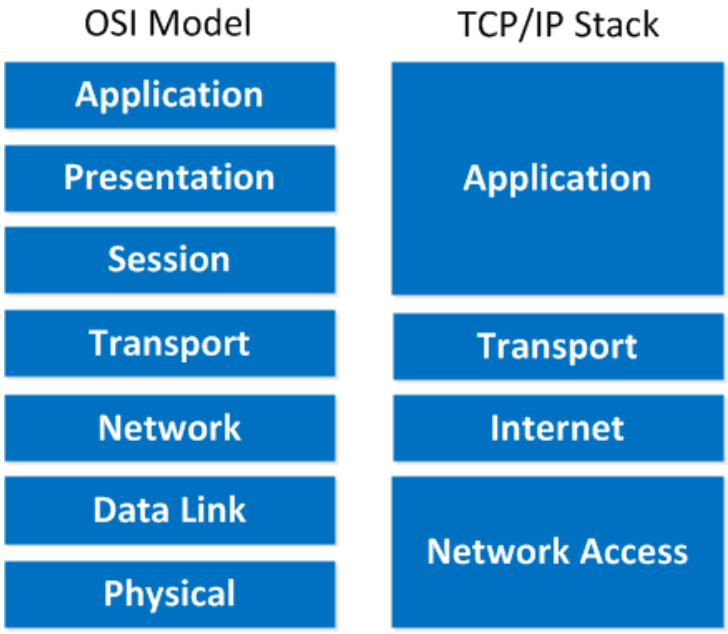
3.2. Sličnosti i razlike TCP/IP modela i OSI RM

OSI referentni model opisuje arhitekturu mreže kako bi računala različitih proizvođača mogla komunicirati. Referentni model predstavlja sve procese potrebne za uspješnu komunikaciju i dijeli sve procese u slojeve. Namjena OSI modela je bila pomoći proizvođačima da naprave kompatabilne mrežne uređaja i softvere u formi protokola. On opisuje kako jedna aplikacija na jednom računalu šalje podatke i mrežne informacije aplikaciji na drugom računalu. Slojevi unutar jednog modela komuniciraju samo s prvim slojem iznad i prvim slojem ispod sebe.[16] OSI referentni model je apstraktni, slojeviti model koji služi kao preporuka stručnjacima za promatranje i za razvoj mreža i protokola, dok je TCP/IP model na kojem se zasnivaju sva današnja računala i Internet.

TCP/IP je slojeviti model koji je dobio naziv po dva bitna protokola: TCP protokolu, te prema IP protokolu. TCP/IP omogućuje komunikaciju više različitih međusobno povezanih mreža i danas je najrasprostranjeniji i najvažniji protokol na lokalnim mrežama.

OSI i TCP/IP model imaju dosta zajedničkog, budući da se oba dva modela temelje na konceptu slojeva nezavisnih protokola, a funkcionalnosti slojeva su dosta slične. Oba modela koriste slojeve za prikaz komunikacije i ti slojevi imaju slične uloge. Oba sloja koriste *packet-switched* tehnologiju, koja opisuje slanje podataka u malim zapakiranim jedinicama podataka zvanima paket. Paketi se usmjeravaju po mreži koristeći odredišnu adresu. Kod OSI modela i kod TCP/IP modela transportni sloj i slojevi na niže pružaju *end-to-end* prijenosnu uslugu procesima koji žele komunicirati, dok su slojevi iznad transportnog aplikacijski orijentirani korisnici transportne usluge.

[16] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_3.pdf



Slika 3. Prikaz OSI modela i TCP/IP modela[17]

Najveća razlika između dva modela je broj slojeva te njihovi nazivi, kao što je vidljivo na slici 3. OSI model ima sedam slojeva, a TCP/IP model ima četiri sloja. Kada se radi usporedba osnovnih koncepta između modela, OSI model drži do usluga, sučelja i protokola. Svaki sloj radi uslugu za sloj iznad sebe. Usluga prikazuje što sloj radi, odnosno kako funkcionira. Sučelje govori procesima iznad sebe kako da pristupe, te definira parametre i kakvi se rezultati mogu očekivati. Protokoli definiraju funkcije sloja i njihov zadatak. OSI model doprinosi razlikovanjem ova tri koncepta. TCP/IP ne pravi razliku između ovih koncepta što rezultira time da su protokoli u OSI modelu bolje sakriveni i da ih je moguće lako zamijeniti kako se tehnologija mijenja. OSI model je dizajniran prije odgovarajućih protokola što znači da model nije namijenjen samo jednoj skupini protokola, ali je loša strana što se u vrijeme dizajna i izrade OSI modela nije bolje razradilo koju funkcionalnost staviti u koji sloj. Kod TCP/IP modela prvo su postojali protokoli pa je na njihovoj osnovi napravljen model. Još jedna bitna razlika je što OSI model podržava i konekcijski-orijentiranu i nekonekcijski-orijetiranu komunikaciju u mrežnom sloju, ali samo konekcijski-orijentiranu u transportnom sloju. TCP/IP podržava oba načina komunikacije u transportnom sloju ostavljajući taj izbor na korisniku, ali posjeduje samo konekcijski-orijentiranu u mrežnom sloju. Postupak pakiranja podataka kod

[17] https://networklessons.com/cisco/tcpip-stack-tutorial/

oba modela je isti, tj. svaki od slojeva unutar OSI ili TCP/IP modela ima neki oblik pakiranja podataka.[18]

[18] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_3.pdf

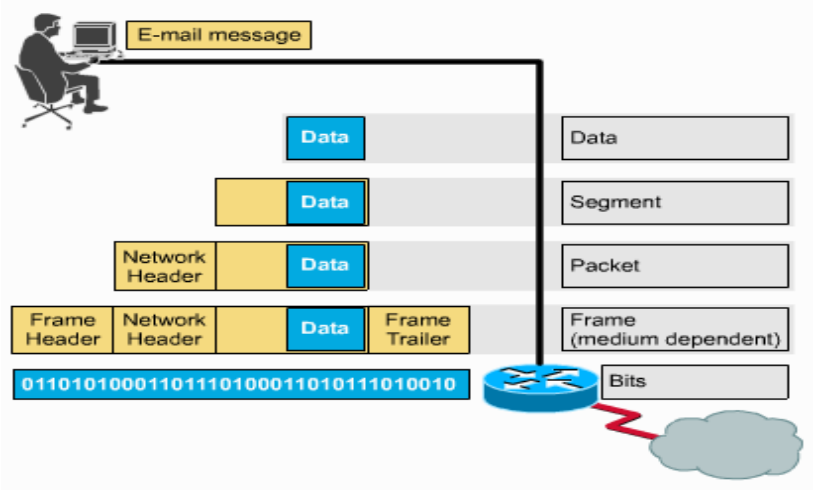
4. Enkapsulacija podataka

Informacije s predajne strane od svojeg pošiljatelja putuju do svojeg cilja, odnosno primatelja, te takve informacije nazivamo paketi podataka. Ako jedno računalo (host A) pošalje podatak drugom računalu (host B), taj podatak prvo mora proći proces pakiranja, odnosno proces enkapsulacije.

Procesom enkapsulacije na podatak se dodaju dodatne informacije koje su važne protokolu da bi taj podatak mogao uspješno te u cijelosti doći do odredišnog računala. Kako podatak od pošiljatelja putuje kroz slojeve OSI modela prema primatelju, na sebe poprima adrese, *network header* (IP adrese), *frame header* (MAC adrese) i *frame trailer*.[19]

Kod transportnog sloja OSI modela podatak se razbija na manje dijelove koji su lakši za rukovanje, a zovu se segmenti. Na tome sloju se na svaki od tih segmenata dodaje broj kao osiguranje da će primatelj podataka te podatke moći sastaviti po redu kako bi trebali izgledati. Kada segment dođe u mrežni sloj tu mu se dodaje zaglavlje te tada nastaje paket. Paket se nakon toga spušta u idući sloj, u sloj podatkovne veze. U sloju podatkovne veze paketu se dodaje zaglavlje tog sloja te nastaje okvir. Kada podatak u takvom obliku, obliku okvira dođe do fizičkog sloja, podaci se konvertiraju u oblik koji je potreban i koji je optimalan za prijenos kod određenog prijenosnog medija.[20] Opisani proces može se vidjeti na slici 4.

[19] http://tfotovic.tripod.com/Enkapsulacija_podataka.html
[20] Mrvelj, Š.: Autorizirani nastavni materijali - Tehnologija telekomunikacijskog prometa I, Fakultet prometnih znanosti, Zagreb, 2014.

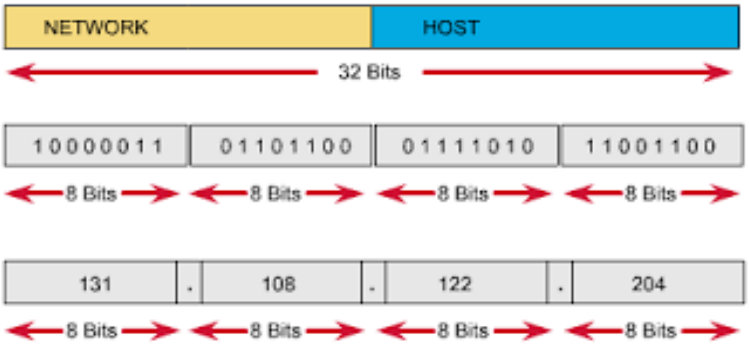


Slika 4. Primjer enkapsulacije podataka[21]

Ako se podaci šalju samo preko lokalne mreže na sebe poprimaju samo MAC adrese jer su samo one potrebne da bi podatak stigao na odredišnu adresu. MAC adresa se može usporediti s našim imenom, dok se network adresa može poistovjetiti s našom poštanskom adresom. Ruteri i računala kao mrežni uređaji imaju MAC adresu i mrežnu adresu. Kada se računalo fizički premjesti u drugu mrežu, to računalo ima istu MAC adresu, samo što mu se mora dodijeliti neka druga network adresa.

Glavna zadaća mrežnog sloja u ovom procesu je da pronađe najbolji put za podatke kroz mrežu, a da bi se to postiglo upotrebljavaju se dva načina adresiranja: flat adresiranje i hijerarhijsko adresiranje. Prvi način adresiranja, flat adresiranje, dodjeljuje svakom uređaju sljedeću slobodnu adresu. Kod drugog načina, najkorištenija verzija hijerarhijskog adresiranja je IP (*Internet Protocol*). Kako informacija prolazi kroz slojeve OSI modela podaci se enkapsuliraju kroz svaki sloj zasebno. Kod mrežnog sloja podaci se spremaju unutar datagrama. IP (*Internet Protocol*) određuje oblik IP zaglavlja koji sadrži adrese i druge kontrolne informacije. IP adresa je dugačka 32 bita, te se sastoji od dva glavna dijela NetID-a i HostID-a. Zbog svoje dužine i nemogućnosti većine ljudi da ih zapamti u binarnom obliku, IP adrese su grupirane u četiri dijela po 8 bita prikazanih u decimalnom obliku i razdvojenih točkom, kao što prikazuje slika 5.[22]

[21] http://tfotovic.tripod.com/Enkapsulacija_podataka.html
[22] http://tfotovic.tripod.com/Enkapsulacija_podataka.html



Slika 5. Primjer izgleda IP adrese[23]

IP adresa sadrži informacije koje su potrebne da bi paket uspješno putovao mrežom. Polje izvorne adrese sadrži IP adresu uređaja koji je poslao podatke, a polje odredišne adrese sadrži IP adresu uređaja koji će primiti podatke.

[23] http://tfotovic.tripod.com/Enkapsulacija_podataka.html

5. Protokoli mrežnog sloja TCP/IP složaja

Za različite načine komunikacije postoje i različite vrste protokola. Protokoli su grupirani u sedam različitih slojeva kod OSI referentnog modela, ili u četiri sloja kod TCP/IP modela. Kod TCP/IP modela protokoli su razvrstani na aplikacijski sloj, transportni sloj, mrežni sloj i sloj podatkovne veze. Način na koji su protokoli podijeljeni po slojevima ovisi o njihovoj zadaći i procesu koji obavljaju na sloju, budući da svaki sloj ima svoju strogo definiranu funkciju, tako i svaki protokol na pojedinom sloju ima svoju funkciju i proces koji mora odraditi u procesu komunikacije. Funkcija svakog sloja je izabrana da zadovolji standardne protokole.

Protokoli se mogu definirati kao skup opće prihvaćenih pravila koja se primjenjuju kod elektroničkog načina prijenosa podataka u nekoj mreži. Protokola ima mnogo po svim slojevima, a da bi se koristili uslugama na Internetu, treba znati njihova značenja, zadaće, procese, prednosti i nedostatke. Mrežni protokol je skup standardnih pravila za prikaz i signalizaciju podataka, te za provjeru od grešaka koju je potrebno izvršiti da bi se podatak uopće poslao. Protokoli mrežnog sloja kod TCP/IP modela podijeljeni su u nekoliko skupina, i to na: kontrolne protokole, protokole razlučivanja adrese, protokole usmjeravanja i internet protokol.

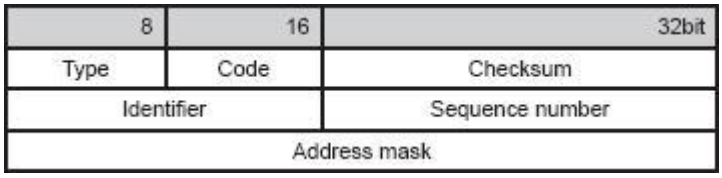
5.1. Kontrolni protokoli

Kontrolni protokoli *Internet Control Message Protocol* (ICMP) i *Internet Group Management Protocol* (IGMP) smatraju se sastavnim dijelovima IP-a, iako koriste IP kao dostavni mehanizam.[24]

ICMP služi za dojavu pogrešaka prilikom usmjeravanja i dostave datagrama, upravljanje prometnim tokom i neke druge funkcije nadgledanja i upravljanja. Osnovna namjena ICMP protokola je osigurati kontrolu prijenosa podataka do odredišta. Ovaj protokol ne osigurava pouzdani prijenos podataka, već to treba osigurati protokol više razine. Poruke se

[24] Bažant, A., Car, Ž., Gledec, G., Jevtić, D., Ježić, G., Kunštić, M., Lovrek, I., Matijašević, M., Mikec, B., Skočir, Z.: Telekomunikacije – tehnologije i tržište, Element, Zagreb, 2007.

šalju samo kao odgovor na poslane IP pakete, a na poslane ICMP pakete odgovor se ne šalje. U slučaju gubitka ICMP poruke, ne generira se nova ICMP poruka o nastaloj pogrešci. ICMP poruke se šalju koristeći osnovno IP zaglavlje, gdje prvi oktet polja podataka IP paketa definira tip ICMP poruke, čime je određen format ostatka paketa, kao što prikazuje slika 6. Osim za dojavu grešaka, ICMP poruke mogu služiti i za slanje drugih informacija.



Slika 6. Format ICMP paketa[25]

ICMP generira osam različitih tipova poruka, a te poruke su: odredište nedostupno, istek vremena, problem s parametrima, blokiranja izvorišta, preusmjeravanje, echo zahtjev/echo odgovor, vrijeme/odgovor o vremenu, zahtjev za informacijom/odgovor na zahtjev za informacijom. Detaljnije objašnjenje ovih poruka nalazi se u nastavku:

- Odredište nedostupno (*Destination Unreachable*) se šalje kada nije moguće uspostaviti vezu ili pronaći put do odredišnog računala, kao i u slučaju kad odredišno računalo ne može prepoznati koja se usluga od njega potražuje. Ako su mreža ili računalo nedostupni, poruku šalje usmjernik, a ako nije prepoznata priključna točka onda ju šalje odredišno računalo.

- Istek vremena (*Time Exceeded*) se šalje kada je paket odbačen jer je polje "TTL" postalo jednako nuli. Ovaj tip poruke se koristi za određivanje puta kroz mrežu.

- Problem s parametrima (*Parametar Problem*) u zaglavlju ne može završiti obradu podataka, te tada paket mora biti odbačen, a poruku generiraju usmjernik ili odredišno računalo.

- Blokiranje izvorišta (*Source Quench*) se generira kada paketi stižu brže nego što ih odredište može obraditi pa usmjernik ili odredišno računalo šalju izvorištu ICMP poruku za privremeni prekid slanja paketa.

[25] http://mreze.layer-x.com/s030300-0.html

- Preusmjeravanje (*Redirection*) je tip koji se provodi kada ICMP poruka koju šalje usmjernik u svojoj tablici usmjeravanja nađe bolji put do odredišta, s tim da se drugi usmjernik mora nalaziti u istoj mreži.

- Echo zahtjev/echo odgovor (*Echo Request/Echo Reply*) je tip koji se koristi kada par poruka kojima se saznaje je li odredište aktivno, u tom slučaju moraju adrese izvorišta i odredišta zahtjeva zamjeniti mjesta u odgovoru.

- Vrijeme/odgovor o vremenu (*Timestamp/Timestamp Reply*) se šalje kada je potrebno saznati za koje vrijeme će se poruka preko odredišta vratiti do izvorišta.

- Zahtjev za informacijom/odgovor na zahtjev za informacijom (*Information Request/Information Reply*) se koristi za doznavanje adrese vlastite mreže.[26]

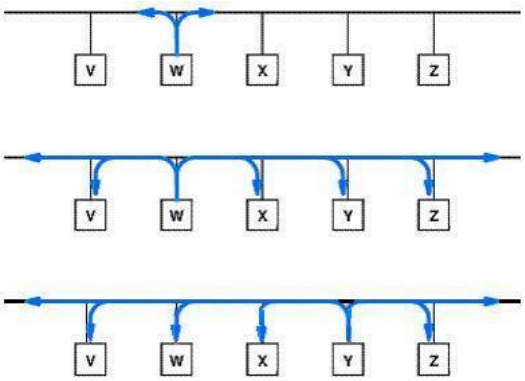
Dok nam prvi kontrolni protokol ICMP služi za dojavu pogreške, drugi protokol ove skupine, IGMP nam služi za prijavu i odjavu sučelja krajnjeg uređaja u skupinu primatelja kod višeodredišnog razašiljanja. Ovaj protokol je komunikacijski protokol koji koriste nositelji i granični usmjerivači na IP mreži. IGMP je protokol na mrežnom sloju TCP/IP složaja koji služi da računalo prijavi svoju prisutnost u multicast skupini na susjednim, udaljenim usmjernicima (*routerima*). *Multicasting* omogućuje jednom računalu na Internetu da šalje sadržaj na više drugih računala koja su sebe identificirala kao računala koja su zainteresirana za primanje takvog sadržaja. *Multicasting* može biti koristan kod računalnih aplikacija kao što su one koje same ažuriraju svoje adresare korisnika mobilnih računala, ili aplikacije koje same šalju novosti neke kompanije na listu distribucije.[27] IGMP se također može koristiti na mrežnim aplikacijama kao što su *online streaming* video i igre, te omogućuje učinkovitije korištenje resursa u trenutku podržavanja ovakvih vrsta aplikacija.

[26] http://mreze.layer-x.com/s030300-0.html
[27] http://searchnetworking.techtarget.com/definition/Internet-Group-Management-Protocol

5.2. Protokoli razlučivanja adrese

Protkoli razlučivanja adrese su ARP (*Address Resolution Protocol*) i RARP (*Reverse Address Resolution Protocol*). Dok je uloga ARP protokola da dobije fizičku adresu na lokalnoj mreži iz poznate IP adrese, uloga RARP protokola je obrnuta, te je taj protokol zadužen da iz poznate fizičke MAC adrese dobije IP adresu.

ARP protokol prevodi IP adresu u MAC adresu, a njegova najraširenija primjena danas je kod protokola Ethernet gdje se IP adrese povezuju s MAC adresama. ARP protokol radi na način da čvor u mreži koji želi dobiti neku MAC adresu razašilje (*broadcast*) ARP zahtjev na mrežu, a čvor u mreži koji ima adresu iz zahtjeva, u odgovoru šalje svoju MAC adresu.

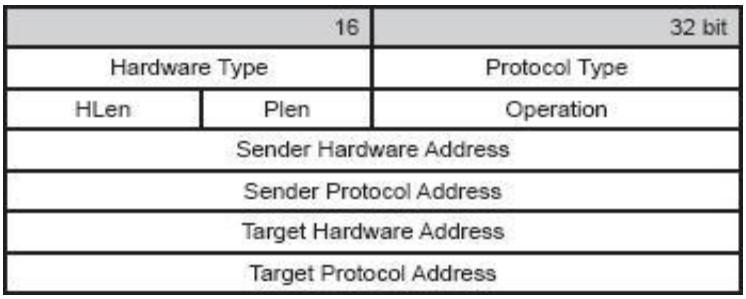


Slika 7. Rad ARP protokola[28]

Preslikavanje između virtualne IP adrese i fizičke adrese se zove pretvaranje adresa (*address resolution*). Računalo ili usmjernik (*router*) koriste prevođenje adresa samo kada šalju pakete unutar iste fizičke mreže, dok se adresa iz daleke fizičke mreže nikada ne prevodi. Postoje tri osnovne tehnike prevođenja adresa, prva tehnika je pretvaranje adrese korištenjem tablice (*table lookup*). Druga tehnika zove se pretvaranje adrese direktnim računanjem (*closed-form computation*), te posljednja tehnika naziva pretvaranje adrese izmjenom poruka (*message exchange*).[29] Kod TCP/IP modela mogu se koristiti sve tri navedene tehnike prevođenja virtualnih adresa. Tehnika pretvaranjem s tablicama se najčešće koristi za prevođenje adresa u WAN-u, dok se tehnika prevođenje izračunavanjem koristi za mreže koje podržavaju

[28] http://mreze.layer-x.com/s020303-0.html
[29] http://web.studenti.math.pmf.unizg.hr/~manger/mr/MrezeRacunala-14.pdf

konfiguriranje fizičkih adresa. Zadnja tehnika prevođenje izmjenom poruka se koristi najčešće u LANovima. ARP protokol se koristi za prevođenje 32-bitnih IP adresa u 48-bitne Ethernet adrese, a specificira se samo opći oblik ARP poruke. Sljedeća slika prikazuje format ARP poruke.



Slika 8. Format ARP poruke[30]

RARP (*Reverse Address Resolution Protocol*) je mrežni protokol pomoću kojega se iz poznate fizičke MAC adrese može saznati IP adresa. RARP protokol se primjenjuje kod sustava bez diska koji prilikom pokretanja ne znaju vlastitu IP adresu pa je dobivaju pomoću RARP upita. Format RARP poruka je sličan ARP formatu. Kada računalo šalje ARP zahtjev, on automatski stavlja svoju hardversku adresu u polje za slanje, te u polje za primanje u enkapsulirani ARP paket podataka. RARP poslužitelj (*server*) će u svom odgovoru na poruku popuniti ispravno slanje i primanje IP adrese. Na taj način će računalo znati svoju IP adresu kada dobije poruku od RARP poslužitelja.[31]

5.3. Protkoli usmjeravanja

Protokoli usmjeravanja se dijele na protokole unutrašnjeg usmjeravanja i protokole vanjskog usmjeravanja. Najčešći protokoli unutrašnjeg usmjeravanja koji su u uporabi su RIP (*Routing Information Protocol*) i OSPF (*Open Shortest Path First*), a protokol za vanjsko usmjeravanje je BGP (*Border Gateway Protocol*).

[30] http://mreze.layer-x.com/s020303-0.html
[31] http://www.comptechdoc.org/independent/networking/guide/netarp.html

RIP (*Routing Information Protocol*) je najstariji usmjerivački protokol koji se primjenjuje na Internetu, razvijen je za lokalne mreže, a zasniva se na razašiljanju (*broadcast*). Ovaj protokol šalje nove usmjerivačke poruke u pravilnim intervalima ili kada se promjeni topologija mreže. Kada usmjernik (*router*) dobije poruku usmjeravanja s promjenama, tablica usmjeravanja se mijenja i nadograđuje da bi prikazala novi put. Kod RIP protokola usmjernici čuvaju samo najbolji put prema odredištu, a ako nova informacija nudi bolji put onda taj novi put zamjenjuje stari. Nakon nadogradnje tablice usmjeravanja, usmjernik informira susjedne usmjernike o promjeni. RIP protokol kao metriku koristi broj skokova te odabire smjer s najmanjim brojem skokova kao najbolji. Broj skokova je broj usmjernika koji paket treba proći na putu do odredišta. Svaki skok na putu od izvorišta do odredišta vrijedi 1, ako nije drugačije definirano, a ako je broj skokova veći od 15 tada se smatra da je odredište nedohvatljivo. RIP ima i mnogo stabilnosnih dodataka koji su zajednički za mnoge usmjerivačke protokole, a te mogućnosti osiguravaju stabilnost zbog potencijalno brzih promjena u topologiji mreže. Najbitnije takve mogućnosti su:

- Podjela obzorja (*Split Horizons*) proizlazi iz činjenice da nije korisno slati informaciju o smjerovima u onom smjeru iz koje smo ju primili. Ovime se sprječava stvaranje usmjerivačkih petlji između dva usmjernika.

- Zadržavanje promjene izbrisanih smjerova (*Hold-Downs*) govori o ažuriranju smjerova koji su prekinuti i ne dolazi istovremeno na svaki usmjernik, pa se može dogoditi da usmjernik koji još nije obaviješten o prekidu veze šalje redovite poruke u kojima navodi da je smjer još ispravan. Usmjernik koji je već obaviješten o prekidu smjera i koji primi takvu poruku, neće odmah takav smjer staviti u svoju tablicu usmjeravanja, već će određeno vrijeme zadržavati promjenu.

- Ažuriranje prekinutih smjerova (*Poison Reverse Updates*) je namijenjeno nalaženju i sprječavanju usmjerivačkih petlji između tri ili više usmjernika, a temelji se na tome da povećanje broja koraka za pojedini smjer obično ukazuje na pojavu usmjerivačke petlje. Stoga se pri uočavanju ovakvih smjerova šalju *poison reverse update* poruke koje brišu takve smjerove iz tablica usmjeravanja.[32]

[32] http://mreze.layer-x.com/s030201-0.html

8	16	32bit
Command	Version	Unused
Address family identifier		Route tag (only for RIP2; 0 for RIP)
IP address		
Subnet mask (only for RIP2; 0 for RIP)		
Next hop (only for RIP2; 0 for RIP)		
Metric		

Slika 9. Format paketa RIPv2[33]

Uz RIP protokol, sljedeći protokol unutrašnjeg usmjeravanja je OSPF (*Open Shortest Path First*) protokol. Ovaj usmjerivački protokol je otvoren, njegove specifikacije su javne, protokol stanja veze koji zahtjeva slanje obavijesti o stanju veze ostalim usmjernicima unutar istog hijerarhijskog prostora. Iako je OSPF unutarnji usmjerivački protokol, sposoban je komunicirati s drugim autonomnim sustavima koji su podijeljeni u područja, a usmjernici mogu biti članovi više područja. Granični usmjernici (*Area Border Routers*) održavaju topološku bazu za svako područje, dok topološka baza sadrži skup LSA-ova svih usmjernika u istom području. Ako su usmjernici unutar istog područja onda imaju jednake topološke baze. Razdvajanje područja stvara dva različita tipa OSPF usmjeravanja, ovisno o tome jesu li izvorište i odredište u istim ili različitim područjima. Intraprostorno usmjeravanje se javlja kada su izvorište i odredište u istom području, a interprostorno usmjeravanje kada su u različitim područjima. Područje okosnice (*Backbone Area*) OSPF-a je odgovorno za distribuiranje usmjerivačkih informacija između područja, sav promet koji povezuje neka druga područja prolazi preko njega. Sva područja moraju biti povezana na područje okosnice i svaki usmjernik unutar područja okosnice zna topologiju cijele mreže.[34]

8	16	32bit
Version No.	Packet Type	Packet length
Router ID		
Area ID		
Checksum		AuType
Authentication (64 bits)		

Slika 10. Format OSPF paketa[35]

[33] http://mreze.layer-x.com/s030201-0.html
[34] http://mreze.layer-x.com/s030202-0.html
[35] http://mreze.layer-x.com/s030202-0.html

Ako postoji veći broj usmjernika u nekom području mora se pronaći način kako optimalno razmijeniti podatke između njih, a kada bi svaki usmjernik slao podatke svim ostalima to bi stvorilo velik broj međusobnih veza i prevelik te nepotreban promet. To se rješava proglašenjem glavnog usmjernika (*Designated Router* - DR) i pomoćnog glavnog usmjernika (*Backup Designated Router* - BDR) za svako OSPF područje mreže, te svaki usmjernik na tom području uspostavlja vezu samo prema DR-u i BDR-u, dok oni preplavljuju mrežu podacima i šalju informacije svim ostalim usmjernicima.

OSPF je dobar za srednje i velike mreže, dok minimalno opterećuje mrežu on omogućava praktički neograničen rast mreže. Ovaj protokol ima i nedostataka. On zahtijeva strukturiranu mrežnu topologiju te je potrebno stručno osoblje koje će brinuti o izgradnji i održavanju mreže. Protokol održava bazu koja treba dosta prostora u memoriji usmjernika, te zahtijeva hijerarhijsku organizaciju mreže, dok ni procesorski zahtjevi nisu zanemarivi.[36]

Protokol za vanjsko usmjeravanje je BGP (*Border Gateway Protocol*) protokol. On je najpopularniji interautonomni sustavski *routing* protokol. Koristi se za usmjeravanje među autonomnim sustavima i trenutačno se koristi u verziji 4, a osnovni algoritam rada BGP protokola je jednostavni DV (*Distance Vector*) protokol. Kada BGP usmjernik sazna prefiks dostupan kroz razne putove, odabire optimalni put, ubacuje ga u svoju tablicu usmjeravanja i objavljuje taj optimalni put ostalim usmjernicima s kojima je izravno spojen. Sam protokol ne pronalazi samostalno susjedne usmjernike, već njih ručno definira administrator mreže. BGP je vrlo kompleksan protokol brojnih mogućnosti koji omogućava mrežnom administratoru detaljan utjecaj na tijekove informacija. Ovaj protokol predstavlja standard za razmjenu informacija između pružatelja internetskih usluga (*Internet Service Provider* - ISP), te između ISP-ova i većih korisnika. Postoje dva tipa BGP protokola, a to su interni BGP (*Interior BGP* - iBGP) i eksterni BGP (*External BGP* - eBGP). Interni BGP (iBGP) koristi se za povezivanje usmjernika unutar istog autonomnog sustava, dok se eksterni BGP (eBGP) koristi za povezivanje različitih autonomnih sustava.

BGP protokol u svom radu koristi četiri tipa poruke: OPEN, UPDATE, KEEPALIVE i NOTIFICATION. Prva poruka, OPEN, se koristi za ostvarivanje sjednice između dva BGP usmjeritelja, a sjednica se temelji na TCP vezi. Tokom te sjednice usmjeritelji mogu izmjenjivati svoje tablice usmjeravanja preko druge vrste poruke, UPDATE poruke. Treći tip

[36] http://sistemac.carnet.hr/node/652

poruke, KEEPALIVE poruka, služi za održavanje sesije, dok se poruka NOTIFICATION šalje u slučaju greške. BGP protokol ima nekoliko nedostataka, a dva najveća su veličina tablica usmjeravanja i slaba sigurnost protokola. Još jedan od nedostataka je problem pojave koja se zove *route flapping*, često izbacivanje i ponovno dodavanje puta zbog krivo podešenog usmjeritelja ili zlonamjernog napada. U tom slučaju dolazi do razmjene velike količine nepotrebnih UPDATE poruka, a BGP usmjeritelj troši vrijeme na njihove obrade. Rješenje je uvođenje vremenske zadrške kod opetovane promjene dostupnosti nekog puta.[37]

5.4. Internet protokol (IP)

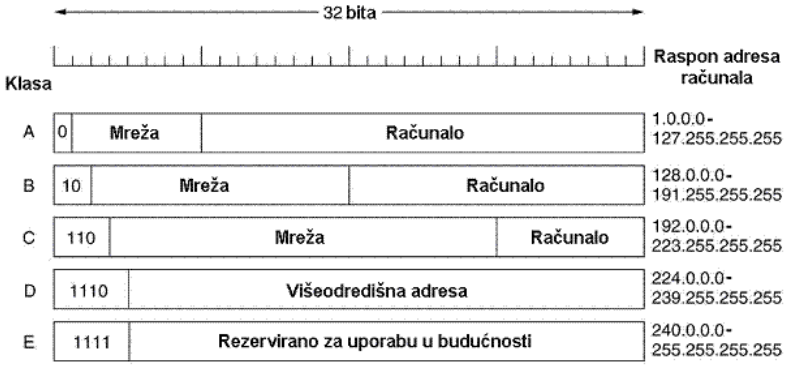
Internet protokol (*Internet protocol* - IP) je mrežni protokol za prijenos podataka kojeg koriste izvorišna i odredišna računala za uspostavu podatkovne komunikacije preko računalne mreže. Podatci u IP mreži se šalju u blokovima koji se nazivaju paketi ili datagrami, a prilikom slanja paketa između izvorišta i odredišta se ne određuje unaprijed točan put preko mreže kojim će podatci putovati, što znači da se IP mreža promatra kao paketska mreža. Ovaj protokol je temeljni protokol na mrežnom sloju TCP/IP modela, te ga koriste protokoli svih viših slojeva. IP je bespojni protokol, što znači da između izvorišta i odredišta nema dogovora o početku ili završetku prijenosa podataka, već kada se paket pošalje s izvorišta prema odredištu, nema nikakve povratne informacije ili potvrde o prijemu paketa. Tek protokoli na višim slojevima provjeravaju konzistentnost podataka, te oni obavljaju detekciju i korekciju pogreški. Zbog takvog načina funkcioniranja ovog protokola, dobio je naziv „nepouzdani protokol“.

Osnovne funkcije IP protokola su: definiranje sheme adresiranja na Internetu, definiranje IP paketa, prosljeđivanje podataka između razine pristupa mreži i prijenosne razine, te fragmentacija i sastavljanje paketa. Glavna zadaća i temeljna funkcija mrežnog sloja je usmjeravanje paketa od izvorišta do odredišta na osnovu IP adrese prijemnika paketa. [38]

IP adresa je jedinstvena adresa svakog računala, uređaja ili mrežnog sučelja spojenog na mrežu. Uređaji koji imaju više sučelja prema mreži imaju po jednu IP adresu za svako sučelje. IP adresa se sastoji od dva dijela: adrese mreže (*network adress*) i adrese računala (*host address*). Adresa mreže identificira podmrežu, dok adresa računala identificira računalo unutar

[37] http://www.cis.hr/dokumenti/bgp-protokol.html
[38] http://mreze.layer-x.com/s030100-0.html

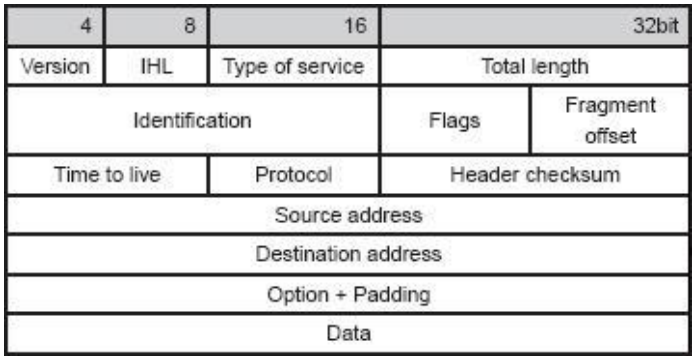
podmreže. IP adresa je binarni broj, koji je kod verzije četiri IP protokola, binarni broj dug 32 bita. Radi lakšeg pamćenja IP adrese one se zapisuju u dekadskom načinu, gdje je 32-bitni broj podijeljen na četiri 8-bitna broja. Ti brojevi se prikazuju kao četiri decimalna broja odvojena točkom. Kod sljedeće verzije IP protokola, IPv6 verzije, predviđaju se 128-bitne adrese. IP adrese mogu biti privatne i javne. Dok su javne IP adrese jedinstvene, globalne i standardizirane, daljnjim razvojem Interneta počelo je nedostajati slobodnih IP adresa. Tako su se razvile privatne IP adrese, koje mogu biti duplicirane uz uvjet da se ne nalaze u istoj lokalnoj mreži. IP adrese su grupirane u pet mrežnih klasa A, B, C, D i E, kao što je vidljivo na slici 11.



Slika 11. Klase IP adresa[39]

Osim funkcije adresiranja, IP omogućuje i specifikaciju vrste usluge, fragmentaciju i ponovno sastavljanje fragmenata, te specifikaciju posebnih mogućnosti, kao što je izvorno usmjeravanje i sigurnost. Ovaj protokol ne sadrži funkcije za upravljanje tokom, održavanje redoslijeda informacijskih jedinica i retransmisiju, koje bi povećale pouzdanost, već se te funkcije izvršavaju na višim slojevima. Internet protokol brine isključivo o „najboljoj mogućoj" isporuci datagrama, a zaštitni kod koristi samo za otkrivanje i odbacivanje datagrama s pogreškom.[40]

[39] http://mreze.layer-x.com/s030101-0.html
[40] Bažant, A., Car, Ž., Gledec, G., Jevtić, D., Ježić, G., Kunštić, M., Lovrek, I., Matijašević, M., Mikec, B., Skočir, Z.: Telekomunikacije – tehnologije i tržište, Element, Zagreb, 2007.



Slika 12. Format IP paketa[41]

IP paket sadrži IP zaglavlje i podatkovno polje, a značenja polja IP paketa su vidljiva na slici 12., te su opisana u nastavku:

- Verzija IP protokola *(Version)* određuje format zaglavlja.
- IHL (*Internet Header Length*) je duljina IP zaglavlja u 32-bitnim riječima, omogućava određivanje početka podataka.
- Tip usluge (*Type of Service*) omogućava usmjernicima različit tretman pojedinih paketa u cilju postizanja zadovoljavajuće kvalitete usluge.
- Ukupna duljina (*Total Length*) IP paketa u oktetima, koja uključuj IP zaglavlje i podatke.
- Identifikator paketa (*Identification*) je važan pri povezivanju svih fragmenata u paket.
- Kontrolne zastavice **(***Flags*) definiraju je li fragmentacija dopuštena i ako jest, ima li još fragmenata istog paketa.
- Mjesto fragmenta (*Fragment Offset*) definira mjesto fragmenta u originalnom paketu.
- TTL (*Time to Live*) je maksimalno vrijeme života paketa u mreži, nakon čega se neisporučeni paket odbacuje, a mjeri se u sekundama.
- Protokol (*Protocol*) označava protokol više razine kojem se podaci prosljeđuju.
- Kontrolni zbroj zaglavlja (*Header Checksum*) se ponovno obračunava i provjerava pri svakoj promjeni podataka u zaglavlju.
- Adresa izvorišta (*Source Address*) je IP adresa predajnika paketa.
- Adresa odredišta (*Destination Address*) je IP adresa prijemnika paketa.
- Opcije (*Options*) sadrže kontrolne informacije o usmjeravanju i sigurnosne parametre.

[41] http://mreze.layer-x.com/s030100-0.html

- Punjenje (*Padding*) je varijabilna duljina, dopuna polja s nulama.[42]

Standard Interneta i najraširanija verzija internet protokola (IP) je verzija četiri (IPv4). IPv4 koristi 32-bitnu IP adresu, zbog prevelike iskoristivosti slijedeća je verzija šest (IPv6), koja koristi 128-bitnu adresu. Ove dvije verzije se razlikuju u načinu adresiranja, ali i brojnim drugim detaljima.

[42] http://mreze.layer-x.com/s030100-0.html

6. Komparacija IPv4 i IPv6 usmjeravanja

Internet Protokol verzije 6 (IPv6) zamjenjuje Internet Protokol verzije 4 (IPv4) kao Internet standard, te je sljedeća evolucija Internet protokola. Većina Internet komunikacije i dalje koristi IPv4 i taj protokol je pouzdan i fleksibilan već preko 20 godina, no on ima ograničenja koja mogu uzrokovati probleme prilikom proširenja mreže. IPv6 je nova, ažurirana verzija IPv4 i postepeno je zamjenjuje kao Internet standard. To se odnosi na nedostatak IPv4 adresa koje su potrebne za sve nove uređaje koje se priključuju na Internet mrežu. Osnovno i najbitnije u poboljšanju IPv6 je proširenje IP adresa od 32 bitova na 128 bitova, omogućujući skoro neograničene jedinstvene IP adrese. Kako sve više ljudi koristi prijenosna računala kao što su mobilni telefoni i ručna računala, povećani zahtjevi bežičnih korisnika doprinose iscrpljivanju IPv4 adresa. Ovakva proširena sposobnost IPv6 adresiranja daje rješenje problema iscrpljenih adresa, te daje dovoljno IP adresa za rastući broj bežičnih uređaja.

IPv6 osigurava nove funkcije koje pojednostavljuju zadatke konfiguriranja i upravljanja adresama u mreži. Svojstvo autokonfiguracije IPv6 automatski konfigurira adrese sučelja i *default* smjerove, te uzima adresu kontrole pristupa mediju uređaja i prefiks mreže koje osigurava lokalni usmjerivač i kombinira te dvije adrese za kreiranje nove, jedinstvene IPv6 adrese. Ako se koristi IPv6 ne treba ponovno numerirati adrese uređaja kada se promijeni dobavljač Internet usluga, jer se ono uglavnom izvodi automatski.[43]

IPv6 rješava mnoge nedostatke IPv4, kao što je broj raspoloživih adresa, dodjela adrese, njezin životni vijek, opseg i tip adrese, brzina, jednostavnost konfiguracije, mobilnost, sustav imena domene, odlomci, sučelje, IP zaglavlje, prosljeđivanje i filtriranje paketa, privatne i javne adrese, pokretanje i zaustavljanje te još mnogo važnih faktora.

Najbitnija razlika između ove dvije verzije je broj raspoloživih adresa, jer kod IPv4 adresa je duga 32 bita (4 bajta) i sastavljena je od mrežnog dijela i dijela hosta, koji ovise o klasi adrese. Ukupni broj IPv4 adresa je 4 294 967 296. Kod IPv6 adresa je duga 128 bitova (16 bajtova), a osnovnu arhitekturu čine 64 bita za broj mreže i 64 bita za broj hosta. Često je host dio IPv6 adrese izveden od MAC adrese ili drugog identifikatora sučelja. IPv6 ima

[43] http://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_61/rzai2/rzai2ipv6whatis.htm?lang=hr

kompliciraniju i složeniju arhitekturu od IPv4 i njezin broj adresa je 10^{28} puta veći od broja IPv4 adresa. Točan broj je 79 228 162 514 264 337 593 543 950 336.[44]

Životni vijek nije primjenjiv kod IPv4 adresa, osim za adrese koje su dodijeljene upotrebom DHCP-a, dok kod IPv6 adrese imaju dva životna vijeka, preferirani i važeći. Preferirani životni vijek je uvijek manji ili jednak važećem životnom vijeku i nakon njegovog isteka adresa se ne treba koristiti kao izvorna IP adresa za neke nove veze ako je dostupna dobra preferirana adresa.

Opseg adresa kod IPv6 je dio arhitekture i *unicast* adrese te imaju dva definirana opsega, uključujući lokalnu i globalnu vezu, dok *multicast* adrese imaju 14 opsega. Kod IPv4 za jednosmjerne adrese ovaj koncept se ne može primijeniti, jer postoji određeni raspon privatnih adresa i *loopback* te se pretpostavlja da su adrese globalne.

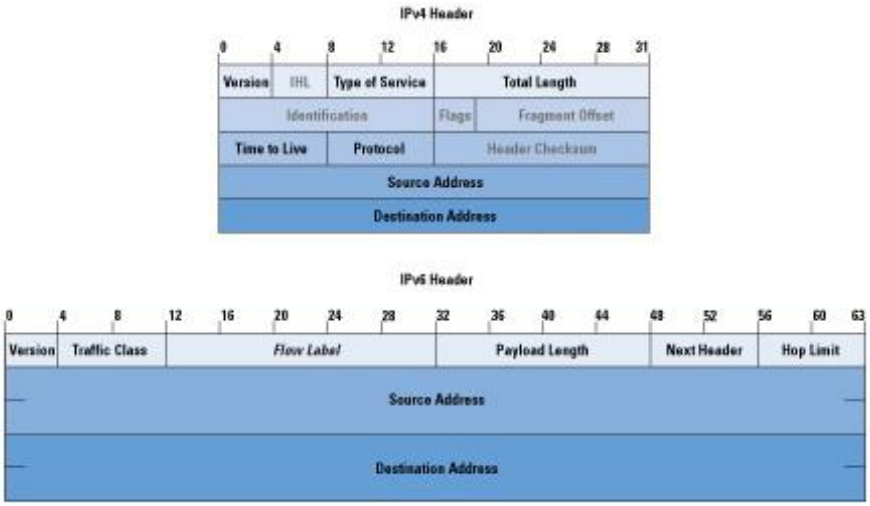
Tipovi adrese se kod IPv4 adresa kategoriziraju u tri osnovna tipa: jednosmjerna adresa, višesmjerna adresa ili univerzalna adresa. Kod IPv6, adrese se kategoriziraju također u tri osnovna tipa: jednosmjerna adresa, višesmjerna adresa i adresa najbližeg odredišta.

Konfiguriranje kod IPv4 je potrebno raditi kod novo instaliranog sustava prije nego može komunicirati s drugim sistemima, što znači da IP adrese i smjerovi moraju biti dodijeljeni. Kod IPv6 konfiguracija nije obavezna, ovisno o traženim funkcijama, jer su IPv6 sučelja samo-konfigurirajuća.

Što se tiče privatnosti, odnosno javnosti adresa, sve IPv4 adrese su javne, osim tri raspona adresa koje su bile označene kao privatne, dok se domene privatnih adresa obično koriste unutar organizacija. Kod IPv6 adrese su javne ili privremene, dok privremene adrese mogu biti globalno usmjerene ali bi trebale štititi identitet klijenta kada on započinje komunikaciju. Privremene adrese imaju ograničeni životni vijek i one se općenito ne razlikuju od javnih adresa.

Filtriranje paketa je osnovna funkcija vatrozida integrirana u TCP/IP kod IPv4, dok IPv6 ne podržava filtriranje paketa. Kod IPv4 se može konfigurirati da prosljeđuje IP pakete koje prima za nelokalne IP adrese, dok IPv6 ima ograničenu podršku za prosljeđivanje paketa.

[44] http://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_61/rzai2/rzai2compipv4ipv6.htm?lang=hr



Slika 13. Format zaglavlja IPv4 i IPv6[45]

IP zaglavlje kod IPv4 je varijabilne dužine od 20-60 bajtova, ovisno o prisutnim IP opcijama, dok je kod IPv6 ono fiksne dužine od 40 bajtova, te mnogo jednostavnije nego kod IPv4, kao što je vidljivo na slici 13.

[45] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_93/ipv6_internals.html

7. Zaključak

Danas, u 21. stoljeću, život je nezamisliv bez pristupa i korištenja Interneta. Koristimo ga svakodnevno i u svim mogućim situacijama, „spajamo“ se na njega mobilnim uređajima, svojim osobnim računalima ili uređajima u svojim automobilima. Zbog tako velikog korištenja Interneta, svakodnevno sve više i više ljudi žele biti i ostati povezani sa svojim prijateljima, obiteljima i znancima. Svakodnevne objave na popularnim društvenim mrežama, slanje video i audio zapisa, slanje tekstualnih poruka, sve to nam omogućuju protokoli koji su sadržani i opisani na mrežnom sloju TCP/IP modela. Taj model prikazuje slojevitu strukturu internetske arhitekture, a mrežni, ili internet sloj čija je glavna funkcija da pruži uslugu povezanosti i odabere najbolju rutu za paket podataka kroz mrežu. Uz funkciju uspostavljanja, održavanja i raskida veze, obavlja još niz procesa, kao što je adresiranje i usmjeravanje, budući da podaci od pošiljatelja do primatelja mogu mrežom putovati različitim rutama.

Protokoli ovog sloja podijeljeni su u četiri skupine. U prvu skupinu spadaju kontrolni protokoli (ICMP i IGMP) koji služe za dojavu pogrešaka prilikom usmjeravanja i dostave datagrama, upravljanje tokom i vrše funkcije nadgledanja i upravljanja. Druga skupina su protokoli razlučivanja adrese (ARP i RARP) koji imaju ulogu da iz poznate IP adrese dobe fizičku MAC adresu i obratno. Iduća skupina su protokoli usmjeravanja, koji se dijele na protokole unutrašnjeg usmjeravanja (RIP i OSPF) i protokole vanjskog usmjeravanja (BGP). Najvažniji, najbitniji i najpoznatiji protokol mrežnog sloja je IP protokol. To je protokol mrežnog sloja koji služi za prijenos podataka kojeg koriste izvorišna i odredišna računala za uspostavu podatkovne komunikacije preko računalne mreže, a razvijen je u dvije verzije: IPv4 i IPv6 koji tek polako dolazi u uporabu, zbog svoje bitne karakteristike, a to je veći broj raspoloživih IP adresa za mrežne uređaje.

Popis literature

[1] Bažant, A., Car, Ž., Gledec, G., Jevtić, D., Ježić, G., Kunštić, M., Lovrek, I., Matijašević, M., Mikec, B., Skočir, Z.: Telekomunikacije – tehnologije i tržište, Element, Zagreb, 2007.: 237-254

[2] Bažant, A., Gledec, Ilić, Ž., Ježić, G., Kos, M., Kunštić, M., Lovrek, I., Matijašević, M., Mikec, B.: Osnovne arhitekture mreža, Element, Zagreb, 2004.: 109-117

[3] Hunt, C.: TCP/IP Network Administration, O'Reilly Media, 1997.: 1-50

[4] Mrvelj, Š.: Autorizirani nastavni materijali - Tehnologija telekomunikacijskog prometa I, Fakultet prometnih znanosti, Zagreb, 2014.

[5] Markežić, I.: Separati s predavanja – Mobilni komunikacijski sustavi, Fakultet prometnih znanosti, Zagreb, 2014.

[6] http://sistemac.carnet.hr/node/352 (03.08.2015.)

[7] http://mreze.layer-x.com/s010100-0.html (03.08.2015.)

[8] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_1_2.html (03.08.2015.)

[9] http://www.konides.ag.rs/mreze/12-OSI/arhitektura_slojeva.html (04.08.2015.)

[10] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_1_3.html (04.08.2015.)

[11] http://tfotovic.tripod.com/ni_protokoli.htm (06.08.2015.)

[12] http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_3.pdf (06.08.2015.)

[13] http://mreze.layer-x.com/s010200-0.html (08.08.2015.)

[14]https://www.certificationkits.com/cisco-certification/ccna-articles/cisco-ccna-standardinternetworking-models/ccna-the-tcpip-suite/ (08.08.2015.)

[15] https://networklessons.com/cisco/tcpip-stack-tutorial/ (08.08.2015.)

[16] http://tfotovic.tripod.com/Enkapsulacija_podataka.html (10.08.2015.)

[17] http://mreze.layer-x.com/s030300-0.html (11.08.2015.)

[18] http://searchnetworking.techtarget.com/definition/Internet-Group-Management-Protocol (13.08.2015.)

[19] http://mreze.layer-x.com/s020303-0.html (13.08.2015.)

[20] http://web.studenti.math.pmf.unizg.hr/~manger/mr/MrezeRacunala-14.pdf (16.08.2015.)

[21] http://www.comptechdoc.org/independent/networking/guide/netarp.html (16.08.2015.)

[22] http://mreze.layer-x.com/s030201-0.html (16.08.2015.)

[23] http://mreze.layer-x.com/s030202-0.html (20.08.2015.)

[24] http://sistemac.carnet.hr/node/652 (20.08.2015.)

[25] http://www.cis.hr/dokumenti/bgp-protokol.html (23.08.2015.)

[26] http://mreze.layer-x.com/s030100-0.html (23.08.2015.)

[27] http://mreze.layer-x.com/s030101-0.html (23.08.2015.)

[28]http://www01.ibm.com/support/knowledgecenter/ssw_ibm_i_61/rzai2/rzai2ipv6whatis.htm?lang=hr (25.08.2015.)

[29]http://www01.ibm.com/support/knowledgecenter/ssw_ibm_i_61/rzai2/rzai2compipv4ipv6.htm?lang=hr (25.08.2015.)

[30]http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_93/ipv6_internals.html (25.08.2015.)

Popis kratica

ARP (*Address Resolution Protocol*)

ASP (*AppleTalk Session Protocol)*

ATM (*Asynchronus Transfer Mode*)

BDR (*Backup Designated Router*)

BGP (*Border Gateway Protocol*)

DARPA (*Defense Advanced Research Projects Agency*)

DoD (Department of Defense)

DR (*Designated Router*)

DV (*Distance Vector*)

eBGP (*External* BGP)

FTP (*File Transfer Protocol*)

HTTP (*HyperText Transfer Protocol*)

iBGP (*Interior* BGP)

ICMP (*Internet Control Message Protocol*)

IGMP (*Internet Group Management Protocol*)

IMAP (*Internet Message Access Protocol*)

IP (*Internet Protocol*)

IPv4 (*Internet Protocol version 4*)

IPv6 (*Internet Protocol version 6*)

ISO (International Organization for Standardization)

LAN (*Local Area Network*)

LLC (*Logical Link Control*)

MAC (*Media Access Control*)

MAN (*Metropolitan Area Network*)

MIL STD (*Military Standards*)

NFS (*Network File System*)

OSI RM (*Open Systems Interconnection Reference Model*)

OSPF (*Open Shortest Path First*)

POP (*Post Office Protocol*)

RARP (*Reverse Address Resolution Protocol*)

RIP (*Routing Information Protocol*)

SMTP (*Simple Mail Transfer Protocol*)

SNMP (*Simple Network Management Protocol*)

TCP (*Transmission Control Protocol*)

TCP/IP (*Transmission Control Protocol/Internet Protocol*)

UDP (*User Datagram Protocol*)

WAN (*Wide Area Network*)

Popis slika